AMENDMENTS TO THE CLAIMS

1.   (Canceled).

2.   (Previously Presented) The electronic voting method of claim 31 or 32, which comprises, prior to the step (d), the additional steps: (d-0) wherein said counter inputs said encrypted vote content and said administrator signature into a signature verification part to make sure that said preprocessed text is signed by said administrator, and publishes a list of vote data containing encrypted vote contents; and (d-1) wherein said each voter makes sure that his encrypted vote content is placed on said list.

3.   (Previously Presented) The electronic voting method of claim 32, wherein: said information randomizing step (a) comprises the additional steps wherein said each voter generates a tag that only he knows, and step wherein said each voter concatenates said encrypted vote content with said tag and randomizes it with said random number; and said step (d-1) comprises the additional step wherein said each voter separates said tag from said vote data on said list and makes a check to see if said tag is his.

4.   (Previously Presented) The electronic voting method of claim 31 or 32, wherein: said step (b) comprises the additional step wherein said administrator publishes, as a list of voters, a list of information representing voters given said blind signature; and said step (c) comprises the additional step wherein said each voter makes a check to see if information representing him is contained in said list of voters.

5.   (Previously Presented) The electronic voting method of claim 31 or 32, wherein said step (d) comprises the additional step wherein said counter publishes the result of counting of said vote content.

6.   (Previously Presented) The electronic voting method of claim 31 or 32, wherein: in said step (a) said each voter sends said preprocessed text to said administrator apparatus together with voter identification information; in said step (b) said administrator verifies the validity of said

each voter on the basis of said voter identification information; and in said step (c) said each voter sends said vote data anonymously to said counter apparatus.

7. (Previously Presented) The electronic voting method of claim 31 or 32, wherein: said step (a) comprises the additional step wherein said each voter generates his signature for said vote content, and sends said his signature to said administrator apparatus together with said vote content; and said step (b) comprises the additional step wherein said administrator apparatus verifies the validity of said voter signature for said vote content.

8-9. (Canceled)

10. (Previously Presented) The electronic voting method of claim 31 or 32, wherein said decryption processing is a thresholding decryption processing that requires a predetermined plural number of said distributed counter apparatuses to work together.

11. (Canceled)

12. (Previously Presented) The electronic voting system of claim 33 or 34, wherein: said each voter apparatus further comprises an administrator signature verification part for verifying the validity of said administrator signature for said information containing said encrypted vote content, and sends said vote data to said counter apparatus when said administrator signature is found valid; and said counter apparatus further comprises an administrator signature verification part into which said information containing said encrypted vote content in said vote data received from said each voter apparatus and said administrator signature are input for verifying the validity of said administrator signature.

13. (Previously Presented) The electronic voting system of claim 33 or 34, wherein: said each voter apparatus further comprises a voter signature generator for generating a voter signature for said preprocessed text and for sending it to said administrator apparatus; and said administrator apparatus further comprises a voter signature verification part for verifying the validity of said preprocessed text received from said each voter apparatus and said voter signature therefore, and

generates said blind signature by said blind signature generator when said preprocessed text and said voter signature are found valid.

14. (Previously Presented) The electronic voting system of claim 33 or 34, wherein: said counter apparatus further comprises a vote list generator which, if said administrator signature is found valid, generates, as a vote list, a list of said vote data received from said each voter apparatus, and publishes said vote list to said voter in a manner to be accessible from said each voter apparatus; and said each voter apparatus further comprises a vote list checker for making a check to see if said encrypted vote content of said each voter apparatus is contained in said vote list received from said counter apparatus.

15. (Original) The electronic voting system of claim 14, wherein said each voter apparatus further comprises: a tag generator for generating a tag that only said voter knows; a concatenator for concatenating said encrypted vote content with said tag to generate information containing said encrypted vote content; and a list checking part for extracting said tag from each vote data in said vote list and for making a check to see if vote data of said voter is contained in said vote list by checking whether said extracted tag is the tag of said voter.

16-17. (Cancelled)

18. (Previously Presented) The electronic voting system of claim 33 or 34, wherein said decryption part performs thresholding decryption processing that requires a predetermined plural number of said distributed counter apparatuses to work together.

19-23. (Cancelled)

24. (Original) The counter apparatus of claim 35 or 36, wherein said partial decryption part performs thresholding decryption processing that requires a predetermined plural number of said distributed counter apparatuses to work together.

25-29. (Cancelled)

Application No.: 09/434,440   Docket No.: 20162-00534-US

30.   (Previously Presented) The recording medium of claim 37 or 38, wherein said step (e) is a step of performing thresholding partial decryption processing that requires a predetermined plural number of said distributed counter apparatuses to work together.

31.   (Previously Presented) An electronic voting method in which voters obtain authorization to vote from an administrator and send their vote data to a counter apparatus, and said counter apparatus performs vote counting, said counter apparatus has a series connection of a plurality of distributed counter apparatuses, each placed under the control of a different counter; a secret key of said counter apparatus is split into partial secret keys assigned to said plurality of distributed counter apparatuses, respectively, said method comprising the steps wherein:

(a) each of said voters encrypts the vote content corresponding to his chosen candidate by an encryptor with a public key of said counter apparatus, and

randomizes information containing said encrypted vote content by a random number to create a preprocessed text, and sends it to an administrator apparatus;

(b) said administrator apparatus verifies the validity of each voter apparatus, and

inputs said received preprocessed text into a signature generator to generate a blind signature for said preprocessed text, and sends it back to said each voter apparatus;

(c) said each voter excludes the influence of said random number from said blind signature for said received preprocessed text; and

obtains a signature of said administrator for said information containing said encrypted vote content, and sends said administrator signature and said information containing said encrypted vote content, as vote data, to one of said plurality of distributed counter apparatuses which is connected to one end of said series connection; and

(d) said plurality of distributed counter apparatuses sequentially decrypt information containing said encrypted vote content in their decryption parts with said partial secret keys to obtain, at the last stage of said series connection, vote content and count at the last stage of said series connection the number of votes polled for the candidate corresponding to said vote content.

5

Application No.: 09/434,440   Docket No.: 20162-00534-US

32.   (Currently Amended) An electronic voting method in which voters obtain authorization to vote from an administrator and send their vote data to a counter apparatus, and said counter apparatus performs vote counting, said counter apparatus has a plurality of distributed counter apparatuses, each placed under the control of a different counter; said secret key is split into partial secret keys assigned to ~~said~~a plurality of distributed counter apparatuses, respectively, said method comprising the steps wherein:

(a) each of said voters encrypts the vote content corresponding to his chosen candidate by an encryptor with a public key of said counter apparatus, and

randomizes information containing said encrypted vote content by a random number to create a preprocessed text, and sends it to an administrator apparatus;

(b) said administrator apparatus verifies the validity of each voter apparatus; and

inputs said received preprocessed text into a signature generator to generate a blind signature for said preprocessed text, and sends it back to said each voter apparatus;

(c) said each voter excludes the influence of said random number from said blind signature for said received preprocessed text; and

obtains a signature of said administrator for said information containing said encrypted vote content, and sends said administrator signature and said information containing said encrypted vote content, as vote data, to all of said plurality of distributed counter apparatuses; and

(d) said plurality of counter apparatuses individually ~~decrypt~~process information containing said encrypted vote content in their decryption parts with said partial secret keys to generate ~~decrypted~~intermediate data, said ~~decrypted~~intermediate data is sent from said distributed counter apparatuses to a predetermined one of them and decrypted into said vote content, and the number of votes polled for the candidate corresponding to said vote content are counted.

33.   (Previously Presented) An electronic voting system which comprises a plurality of voter apparatuses, an administrator apparatus connected to each of said voter apparatuses through a nonanonymous communication channel, and a counter apparatus connected to each of said voter apparatuses through an anonymous communication channel, wherein:

6

Application No.: 09/434,440   Docket No.: 20162-00534-US

said counter apparatus has a series connection of a plurality of distributed counter apparatuses, each placed under the control of a different counter, a secret key of said counter apparatus is split into partial secret keys assigned to said plurality of distributed counter apparatuses, respectively;

said each voter apparatus comprises:

an encryptor for encrypting a vote content of a voter of said each voter apparatus with a public key of said counter apparatus to generate an encrypted vote content;

a random generator for generating a random number;

a randomizer for randomizing said encrypted vote content with said random number to create a preprocessed text;

means for sending said preprocessed text to said administrator apparatus;

a derandomizer for excluding the influence of said random number from a blind signature of said administrator apparatus, received therefrom, for said preprocessed text to obtain an administrator signature of said administrator apparatus for information containing said encrypted vote content; and

- means for sending said administrator signature and said information containing said encrypted vote content, as vote data, to one of said plurality of distributed counter apparatuses which is connected to one end of said series connection;

said administrator apparatus comprises:

a blind signature generator for generating said blind signature for said preprocessed text;

means for sending said blind signature to said each voter apparatus; and

said distributed counter apparatuses comprise:

decryption parts for sequentially decrypting information containing said encrypted vote content with said partial secret keys, said vote content being obtained by the decryption processing in said distributed counter apparatus at the last stage of said series connection; and

a counter provided at the last stage of said series connection, for performing vote counting for each candidate on the basis of said decrypted vote content.

34.   (Currently Amended) An electronic voting system which comprises a plurality of voter apparatuses, an administrator apparatus connected to each of said voter apparatuses through a

7

Application No.: 09/434,440   Docket No.: 20162-00534-US

nonanonymous communication channel, and a counter apparatus connected to each of said voter apparatuses through an anonymous communication channel, wherein:

said counter apparatus has a plurality of distributed counter apparatuses, each placed under the control of a different counter, a secret key of said counter apparatus is split into partial secret keys assigned to said plurality of distributed counter apparatuses, respectively;

said each voter apparatus comprises:

an encryptor for encrypting a vote content of a voter of said each voter apparatus with a public key of said counter apparatus to generate an encrypted vote content;

a random generator for generating a random number;

a randomizer for randomizing said encrypted vote content with said random number to create a preprocessed text;

means for sending said preprocessed text to said administrator apparatus;

a derandomizer for excluding the influence of said random number from a blind signature of said administrator apparatus, received therefrom, for said preprocessed text to obtain an administrator signature of said administrator apparatus for information containing said encrypted vote content;

means for sending said administrator signature and said information containing said encrypted vote content, as vote data, to all of said plurality of distributed counter apparatuses; and

said administrator apparatus comprises:

a blind signature generator for generating said blind signature for said preprocessed text;

means for sending said blind signature to said each voter apparatus; and

each of said distributed counter apparatuses comprises:

a decryption part for ~~decrypting~~processing said encrypted vote content with said partial secret key assigned thereto to generate ~~decrypted~~ intermediate data and for sending said ~~decrypted~~intermediate data to a predetermined one of said distributed counter apparatuses; and

a total decryption part provided in said predetermined distributed counter apparatus for decrypting all of said ~~decrypted~~intermediate data to obtain said vote content; and

a counter provided in said predetermined distributed counter apparatus for performing vote counting for each candidate on the basis of said decrypted vote content.

8

35.   (Previously Presented) A counter apparatus in an electronic voting system which comprises a plurality of voter apparatuses, an administrator apparatus connected to each of said voter apparatuses through a nonanonymous communication channel, and said counter apparatus connected to each of said voter apparatuses through an anonymous communication channel,

said counter apparatus comprising:

an administrator signature verification part supplied with information containing vote content encrypted by a public key of a counter, received as vote data from said each voter apparatus, and an administrator signature for information containing said encrypted vote content, for verifying the validity of said administrator signature;

a vote list generator for generating a list of said vote data received from said each voter apparatus when said administrator signature is found valid and for publishing said list to a voter of said each voter apparatus in a manner to be accessible therefrom;

a decryptor for decrypting said information containing said encrypted vote content with a secret key corresponding to said public key to obtain the vote content of said voter;

counter-means for counting the number of votes polled for each candidate on the basis of said decrypted vote content;

a series connection of a plurality of distributed counter apparatuses, each placed under the control of a different counter, and

wherein: said secret key is split into partial secret keys assigned to said plurality of distributed counter apparatuses, respectively; said vote data sent from said each voter apparatus is received by that one of said plurality of distributed counter apparatuses which is connected to one end of said series connection; said distributed counter apparatuses have partial decryption parts for sequentially decrypting information containing said encrypted content with said partial secret keys, and said vote content is obtained by the decryption process of said partial decryption part in said distributed counter apparatus at the last stage of said series connection.

36.   (Currently Amended) A counter apparatus in an electronic voting system which comprises a plurality of voter apparatuses, an administrator apparatus connected to each of said voter apparatuses through a nonanonymous communication channel, and said counter apparatus

9

Application No.: 09/434,440   Docket No.: 20162-00534-US

connected to each of said voter apparatuses through an anonymous communication channel, said counter apparatus comprising:

an administrator signature verification part supplied with information containing vote content encrypted by a public key of a counter, received as vote data from said each voter apparatus, and an administrator signature for information containing said encrypted vote content, for verifying the validity of said administrator signature;

a vote list generator for generating a list of said vote data received from said each voter apparatus when said administrator signature is found valid and for publishing said list to a voter of said each voter apparatus in a manner to be accessible therefrom;

a decryptor for decrypting said information containing said encrypted vote content with a secret key corresponding to said public key to obtain the vote content of said voter;

counter means for counting the number of votes polled for each candidate on the basis of said decrypted vote content;

a plurality of distributed counter apparatuses, each placed under the control of a different counter, and

wherein said secret key is split into partial secret keys assigned to said plurality of distributed counter apparatuses, respectively; said plurality of distributed counter apparatuses each have a partial decryption part for ~~decrypting~~processing said encrypted vote content with said partial secret key assigned thereto to generate ~~decrypted~~intermediate data and for sending said ~~decrypted~~intermediate data to a predetermined one of said distributed counter apparatuses; and said predetermined distributed counter apparatus has a total decryption part for decrypting all of said ~~decrypted~~intermediate data to obtain said vote content.

37.   (Previously Presented) A recording medium having recorded thereon a program for executing, by a computer, a procedure of a counter apparatus in an electronic voting system which comprises a plurality of voter apparatuses, an administrator connected to each of said plurality of voter apparatuses through a nonanonymous communication channel, and said counter apparatus connected to said each vote apparatus through an anonymous communication channel, wherein said counter apparatus has a series connection of a plurality of distributed counter apparatuses, each placed under the control of a different counter; said secret key is split into

10

Application No.: 09/434,440   Docket No.: 20162-00534-US

partial secret keys assigned to said plurality of distributed counter apparatus s, respectively, said procedure comprising the steps of:

(a) receiving, as vote data, from each of said vote apparatuses information containing a vote content of each voter encrypted with a public key of said counter apparatus and an administrator signature for said information and verifying the validity of said administrator signature;

(b) generating, as a vote list, a list of said vote data received from said each voter apparatus, if said administrator is found valid, and publishing said vote list in the form accessible by said each voter;

(c)   decrypting said information containing said encrypted vote content with a secret key corresponding to said public key to obtain the vote content of said each voter, receiving said vote data sent from said each voter apparatus by that one of said plurality of distributed counter apparatuses which is connected to one end of said series connection, and sequentially performing partial decryption processes of said information containing said encrypted vote content by said distributed counter apparatuses with said partial secret keys assigned thereto, respectively; and said vote content is obtained by said partial decryption process in said distributed counter apparatus at the last stage of said series connection; and

(d) counting the number of votes polled for each candidate on the basis of said decrypted vote content.

38.   (Currently Amended) A recording medium having recorded thereon a program for executing, by a computer, a procedure of a counter apparatus in an electronic voting system which comprises a plurality of voter apparatuses, an administrator connected to each of said plurality of voter apparatuses through a nonanonymous communication channel, and said counter apparatus connected to said each vote apparatus through an anonymous communication channel, wherein said counter apparatus has a plurality of distributed counter apparatuses, each placed under the control of a different counter; said secret key is split into partial secret keys which are assigned to said plurality of distributed counter apparatuses, respectively, said procedure comprising the steps of:

11

Application No.: 09/434,440   Docket No.: 20162-00534-US

(a) receiving, as vote data, from each of said vote apparatuses information containing a vote content of each voter encrypted with a public key of said counter apparatus and an administrator signature for said information and verifying the validity of said administrator signature;

(b) generating, as a vote list, a list of said vote data received from said each voter apparatus, if said administrator is found valid, and publishing said vote list in the form accessible by said each voter;

(c) decrypting said information containing said encrypted vote content with a secret key corresponding to said public key to obtain the vote content of said each voter, receiving said vote data from all of said voter apparatuses by each of said plurality of distributed counter apparatuses, then ~~encrypting~~process said encrypted vote content with said partial secret key assigned to said each distributed counter apparatus to generate ~~decrypted~~ intermediate data, then sending said ~~decrypted~~ intermediate data to said predetermined distributed counter apparatus, and performing, by said predetermined distributed counter apparatus, total decryption processing of all of said ~~decrypted~~ intermediate data sent thereto to thereby obtain said vote content; and

(d) counting the number of votes polled for each candidate on the basis of said decrypted vote content.

12